NIST National Institute of Standards and Technology

Interim Briefing on the NIST NGI Program for the PITAC

Kevin Mills

October 6, 1999

Briefing Outline

- Quick Overview of NIST
- Nine NGI-Related Projects
  - NGI Security (3)
  - NGI Quality of Service (4)
  - NGI Applications (2)
- Inter-Agency Cooperation on NGI
- NGI-Related Technology Transfer
- Summary

NIST

. . . working with industry to develop and apply technology, measurements and standards.

- Advanced Technology Program
- Baldrige Quality Program
- Manufacturing Extension Partnership
- **Measurement and Standards Laboratories**

I'm briefing projects contained within NIST Measurement and Standards laboratories.

Measurement & Standards Laboratories in Action

- Developing Test and Measurement Technology, e.g.,
  - *Research Prototypes of Emerging Networking Standards*
  - *Protocol Test Systems*
  - *Experimentation and Analysis Tools for Network Quality of Service*
- Providing Leadership in Industry Standards Development, e.g.,
  - *Internet Engineering Task Force: IP Security and Public Key Infrastructure*
  - *IEEE 802.14: Hybrid Fiber-Coax*
  - *Optical Internetworking Forum: Reconfigurable Optical Networks*
  - *FIPS: Advanced Encryption Standard*
- Applying Advanced Technology to Assist U.S. Industry, e.g.,
  - *Advanced Collaboration Technology for Manufacturing Chains*
  - *Networked Virtual Environments for Tele-Manufacturing*

Nine NGI-Related Projects

NGI Security

- Internet Security Protocols
- Advanced Encryption Standard
- Public Key Infrastructure

NGI Quality of Service

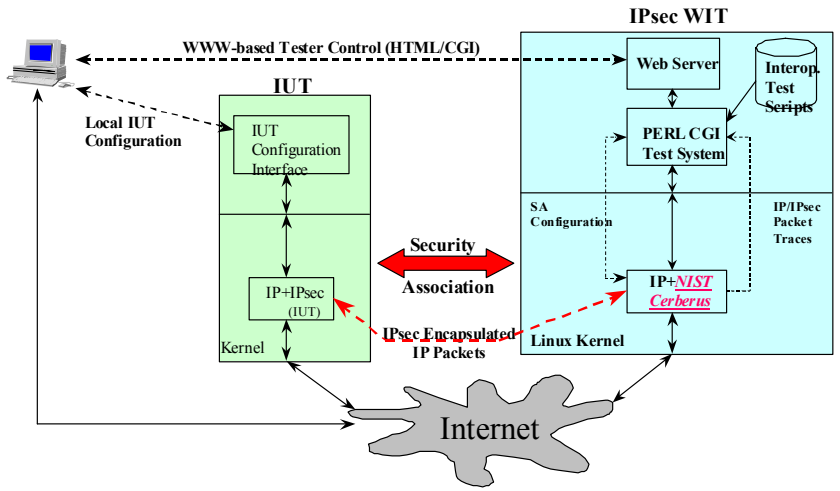
- Internet Quality of Service
- Hybrid Fiber-Coax Access
- Dense Wave-Division Multiplexing
- Agile Networking Infrastructures

NGI Applications

- Manufacturing Collaboratories
- Virtual Manufacturing Interfaces

Internet Security Protocols

"WIT: Web-based IPSec Testing"



Goal

Expedite the commercial deployment of security technology for the next-generation Internet.

Technical Approach

- Expedite development and improve quality of IETF IP Security (IPsec) standards
- Develop research prototypes of emerging IETF IPSec specifications.
- Design and develop automated test technology that will improve the quality and commercial availability of IPSec products.

Customers

- IETF IPSec working groups
- Our test tools and prototypes are being used by 100s of organizations in the Internet research and development community.
- ANX security working group.

Collaborators

- NSA
- INRIA, Korea Telecom
- Cisco, Bay Networks, IBM T.J. Watson, BBN Technologies, NSA, Sable Systems

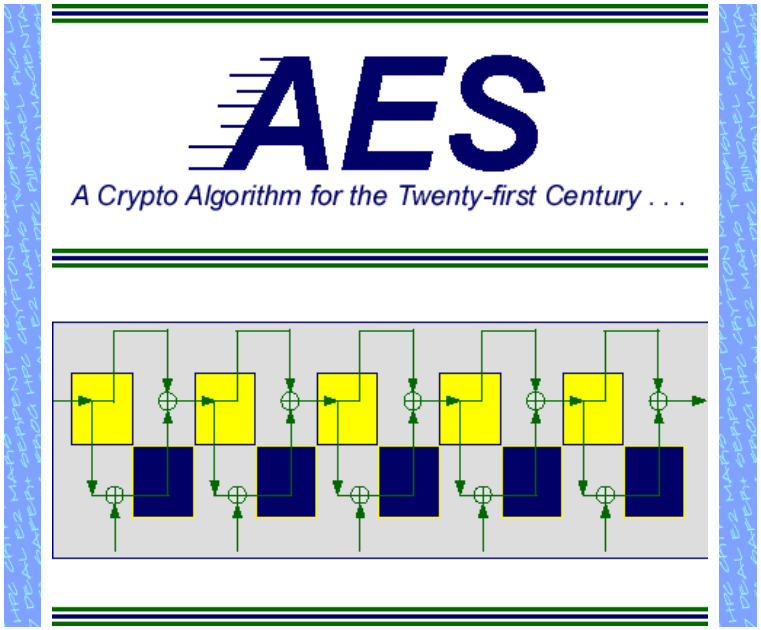
Recent Results

- ***Cerberus/PlutoPlus*** - reference prototype of IETF IPsec and IKE protocols
- ***IPsec-WIT*** - on line, Web-based interoperability test system for IPsec / IKE.

What's Next?

- Expand test systems to address PKIX certificate protocols (FY99)
- Analyze the applicability of IPsec to IPv6 (FY99)
- Prototype and analyze security policy management protocols (FY00)
- Develop formal modeling techniques to assess the security properties and generate test suites for IPsec / IKE / PKIX (FY00)
- Analyze the scalability of IPsec / IKE / PKIX in large scale VPN environments (FY00)

Advanced Encryption Standard



Goal

Develop a new, royalty-free encryption standard that can be used by government and industry to protect information for the next 30-50 years.

Technical Approach

- Efficiency testing of candidate algorithms, using multiple platforms and compilers.
- Consolidation of public and government analysis, comparing efficiency testing results and determining validity of cryptanalysis.
- Validation testing of COTS products for conformance to AES.

Customers

- U.S. banking industry
- U.S. government agencies
- Network users at large

Collaborators

- IBM, Counterpane Systems, RSA Laboratories, Cylink Corporation, TecApro Internacional SA , Future Systems, Inc., Nippon Telephone & Telegraph, Entrust Technologies, Deutsche Telekom, and various academic institutions in the U.S. & abroad.

- National Security Agency (NSA) and Bureau of Export Administration (BXA)

Recent Results

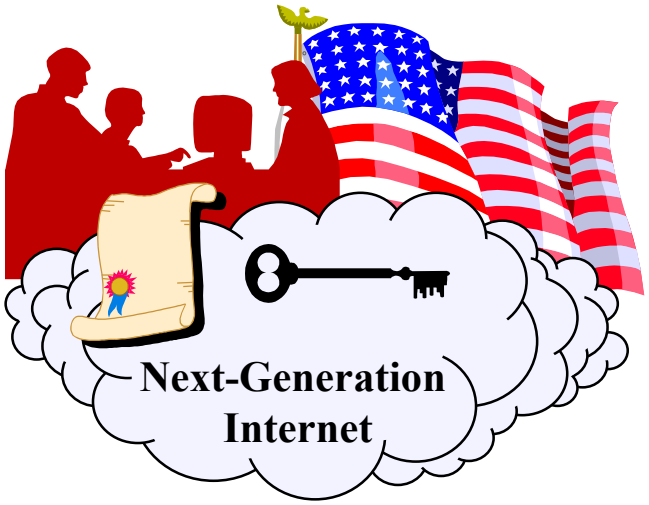
- Hosted Second AES Candidate Conference in March ‘99 to discuss and present Round 1 analysis results.
- Selected 5 algorithms for Round 2 analysis.

What’s Next?

- Perform Round 2 analysis and host Third AES Candidate Conference. (FY99-00)
- Selection of final AES algorithm(s). (FY00)
- Develop FIPS and prepare validation suite to test for conformance of COTS products to AES. (FY01)

Public Key Infrastructure

"The Key to Public Confidence"



Goal

Ensure development of commercially available public key infrastructure (PKI) products and services that are interoperable and are sufficiently secure to meet the needs of government agencies and the general public.

Technical Approach

- Work with users and suppliers to establish PKI standards and specifications; interoperability, correctness, and quality
- Publish analysis of PKI component security requirements and guidance on key management
- Develop pilots for automated key recovery systems and web-based electronic certification

Customers

- PKI component vendors
- PKI product consumers
- Network application and protocol designers.

Collaborators

- AT&T, Baltimore Technologies, CertCo, Certicom, Cylink, Digital Signature Trust, DynCorp, Entrust Technologies, Frontier Technologies, IBM, ID Certify, GTE, Mastercard, Microsoft, Motorola, Netscape, Network Associates, RSA, Spyrus, VeriSign, Visa, World Talk

- Department of Treasury, Federal PKI Steering Committee, Federal agencies participating in Key Recovery Demonstration Project, GITS Board, NSA

Recent Results

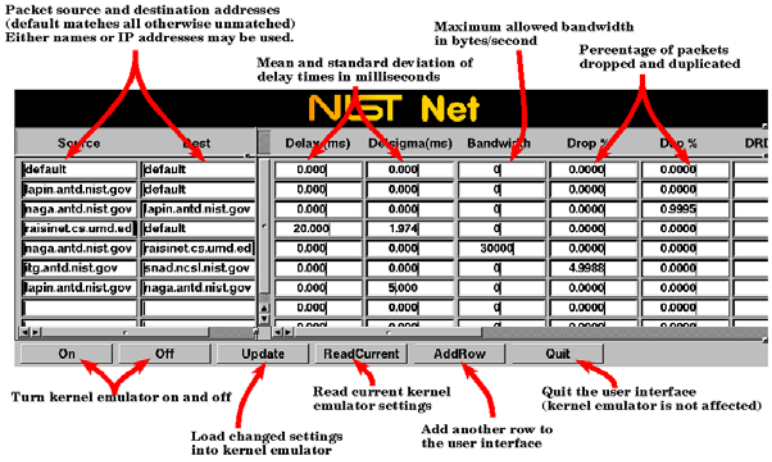
- Developed security requirements for certificate issuing and management components
- Performed PKI interoperability tests based on Minimum Interoperability Specifications for PKI Components （MISPC)

What's Next?

- Develop validation tests for security requirements for PKI components.
- Expand industry participation in PKI interoperability activities.

Internet Quality of Service

"NIST Net: The Internet-in-a-Box"



Goal

Expedite the commercial deployment of standardized Internet Quality of Service (QoS) technologies.

Technical Approach

- Devise tools to aid developers of adaptive Internet applications.
- Research and develop techniques and tools to test and to experiment with distributed multiparty QoS routing and signaling protocols.
- Evaluate proposed algorithms and protocols for scalable QoS routing and signaling.

Customers

- Our test tools and prototypes are being used by 100s of organizations in the Internet research community and the commercial development community.

Collaborators

- DARPA, NIMA, NASA AMES / NREN
- ETRI
- Darmstadt University, Chungnam National University

Recent Results

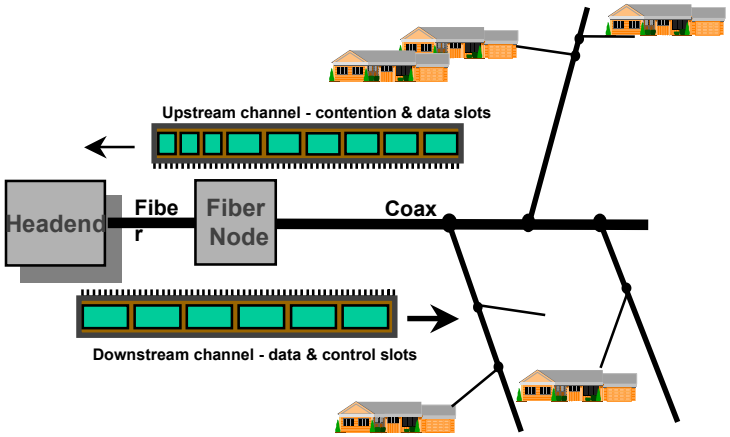
- ***NIST Net*** - tool for emulating controllable Internet performance dynamics
- ***ISPI*** – tools measuring and experimenting with Resource Reservation Protocols

What's Next?

- Release *DIPPER* - Distributed test tool for QoS signaling (FY99)
- Develop *NISTSwitch* - MPLS/QoS routing prototype (FY99)
- Research and development scalable MPLS based QoS routing algorithms (FY00)
- Develop large scale simulation capability for traffic engineering and QoS scaling analysis of MPLS protocols (FY00)

Hybrid Fiber-Coax Access

"Fair, Fast Access from the Home"



Goals

Expedite industry consensus on standard Media Access Control (MAC) protocols for Hybrid Fiber-Coax (HFC) networks.

Technical Approach

- Model and evaluate MAC protocol proposals from IEEE802.14 members.
- Evaluate priority schemes to support Quality of Service.
- Study end-to-end performance issues: improving the effectiveness of ATM and TCP/IP traffic over HFC networks.

Customers

- IEEE 802.14 WG
- Society of Cable Telecommunications Engineers, Inc. (SCTE)
- Cable TV vendors and operators.

Collaborators

- IBM, Zenith Electronics, Scientific Atlanta, LanCity, Com21, 3Com, Motorola, Compaq
- University of Virginia.

Recent Results

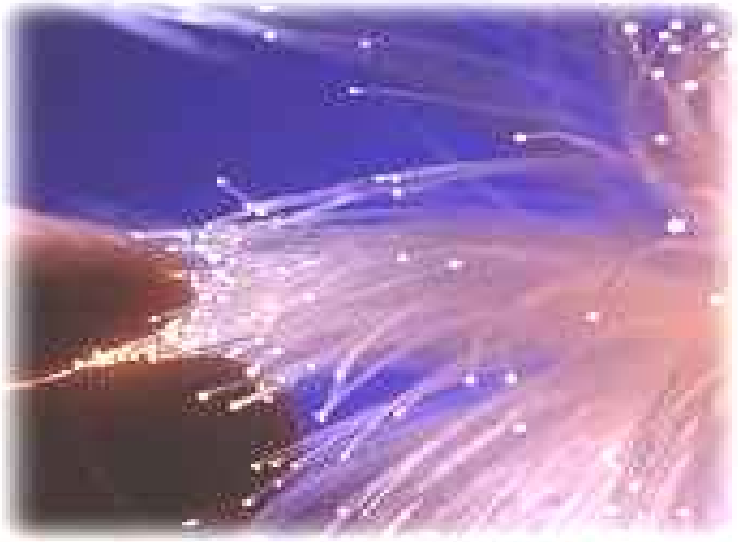
- Enhanced the ***NIST ATM network simulator*** to include HFC network protocols, IEEE802.14 & SCTE.
- Published results on contention resolution algorithms, bandwidth allocation, and priority schemes, on end-to-end performance issues for TCP/IP, ATM traffic control.
- Published reports on performance comparison of IEEE 802.14 and SCTE MAC protocols, and on support of IP QoS on HFC.
- Authored conformance requirements (Annex B) of the IEEE 802.14 standard.

What's Next?

- Nothing – Project has ended.

Dense λ-Division Multiplexing

"Infinite Bandwidth On Demand"



Goal

Accelerate development of technology leading to dynamically reconfigurable Dense Wavelength Division Multiplexing (DWDM) networks.

Technical Approach

- Develop methods to measure output spectra and transient behavior of tunable elements and then characterize the effect of optical signal parameters (e.g., s/n ratio and λ stability) on network behavior.
- Develop hybrid simulation-analytical models for evaluating dynamic λ reconfiguration algorithms.
- Evaluate proposed algorithms for λ assignment and routing in WDM networks.
- Develop a configurable optical network interface card (λ-NIC) to test and evaluate proposed approaches to optical framing

Customers

- Standard organizations: ANSI T1,ITU-T, Optical Internetworking Forum, IETF
- Bell Atlantic and other service providers
- Equipment vendors

Collaborators

- Optical simulation tool designers, vendors (ARTIS, Virtual Photonics,Telcordia)
- DARPA NGI/ONRAMP, MONET teams, Telcordia

Recent Results

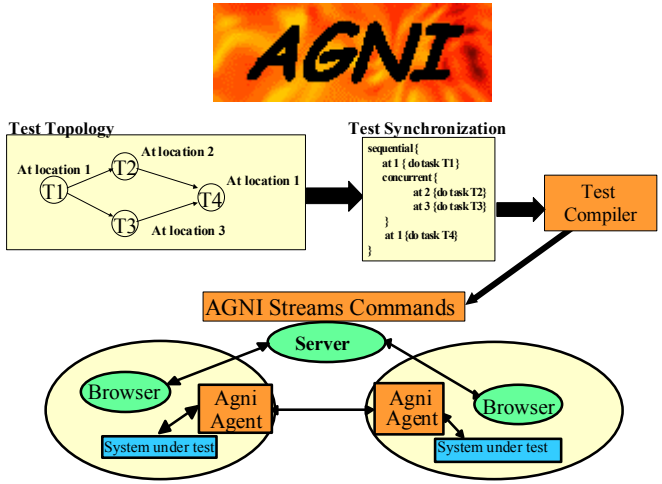
- No results yet - new initiative.

What's Next?

- Assemble monitoring, test and measurement facilities. (FY 99)
- Publish initial measurements of optical signal parameters. (FY 00)
- Develop MERLiN. a WDM network design and modeling environment that integrates existing analytical and simulation models, including ns2 and NIST ATM simulator. (FY99-00)
- Develop λ-NIC. (FY 99-00)
- Design and implement a library of efficient wavelength assignment and routing algorithms. (FY 99-00)
- Publish results of reconfiguration/protection studies. (FY 00)

Agile Networking Infrastructures

"Reconfigurable Networking on the Fly"



Goal

Expedite the development of *agile networking* technologies that enable programmable and reconfigurable communication infrastructures.

Technical Approach

- Research and develop *middleware* technologies for adaptive, reconfigurable distributed systems.
- Evaluate measurement and standardization requirements for networked *pervasive computing* based upon pico-cellular wireless networks and service discovery and composition technologies.
- Develop measurement techniques that enable resource control in *active network* technologies.

Customers

- DARPA, NIST/NAMT
- Middleware & distributed systems R&D community
- CSCW test and evaluation community
- IEEE 802.15, Bluetooth, HomeRF, Sun Java-Jini community

Collaborators

- U. Md, UC Santa Barbra, Old Dominion U.
- NAI Labs, MAYA Design.

Recent Results

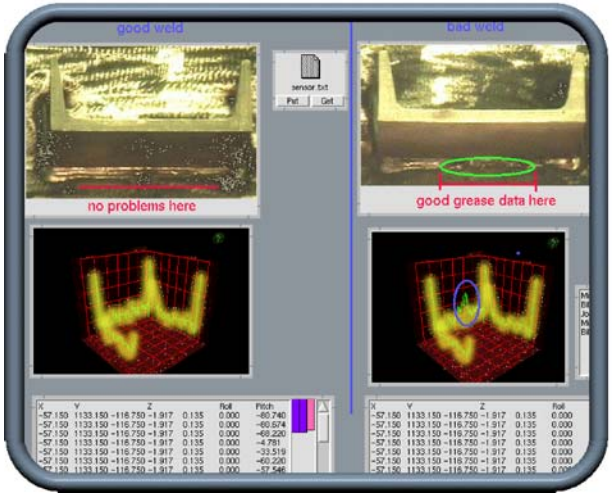
- ***AGNI --*** mobile streams middleware framework and toolkit.
- ***SCAN --*** devised metrics and measurement techniques for Self-Calibrating Active Nodes.

What's Next?

- Prototype development of AirJava adapter and testbed (FY00)
- Prototype SCAN execution environment for Active Nets (FY00)
- Evaluate alternative approaches to service discovery and composition in pervasive computing networks (FY00-01)
- Characterize the internetworking requirements for pervasive computing networks (FY00-01)
- Research and develop technologies for construction of dynamic virtual overlay networks. (FY00-01)

Manufacturing Collaboratories

"Manufacturing Together on the Net"



Goal

Identify gaps in integration and standards for manufacturing activities stemming from use of collaborative environments

Technical Approach

- Deploy manufacturing collaboratory testbed and evaluate collaboration processes
- Deploy and assess a Robotic Arc Welding collaboratory
- Deploy and assess an industrial pilot collaboratory
- Develop quantitative evaluation methods for collaboration technologies

Customers

- Delphi Chassis
- Borg-Warner
- Caterpillar

Collaborators

- Sun Microsystems
- Teamwave Software
- University of Michigan
- University of Saskatchewan

Recent Results

- Deployed a pilot collaboratory for robotic arc welding and published preliminary results on usage
- Integrated commercial CSCW applications, NIST-developed multi-media playback and annotation tools and "SmartRoom" technologies

What's Next?

- Continue evaluation of collaboratory technologies for welding research
- Work with University of Michigan to evaluate distributed, collaborative design of clutch system with Borg-Warner Automotive units in U.S. and Germany

Virtual Manufacturing Interfaces

"Manufacturing from a Distance"

Goal

Prototype and develop interfaces specific to virtual manufacturing applications.

Technical Approach

- Develop testbed for demonstrating real-time multi-user interactive simulation of manufacturing equipment control
- Develop extensions to VRML for device behaviors

Customers

- Searle

Collaborators

- University of Illinois
- National Center for Supercomputing Applications

Recent Results

- Built remote interface to a weld cell with real-time display of a data-driven VRML weld controller model
- Synchronized real-time video with a VRML model

What's Next?

- Link full immersion "cave" environment at University of Illinois to welding robot at NIST via Internet2
- Build a multi-user virtual environment representing human participants at both sites and the welding robot as avatars
- Establish remote control of welding robot through the virtual world

Inter-Agency Cooperation on NGI and Related Networking Programs

Cooperative Projects

- Active Networks Resource Management (with DARPA)
- Adaptive Middleware for Distributed Systems (with DARPA)
- Internet Security Technology (with NSA)
- Advanced Encryption Standard and Public Key Infrastructure (with NSA)
- NGI Demonstrations: SC'98, SC'99, Netamorphosis (with LSN)

Joint Workshops

- Validation of Large-Scale Network Simulations (with DARPA)
- "Bridging the Gap" (organizers with NASA)
- Smart Environments (with NSF and DARPA)

Proposal Reviews

- DARPA Proposals: NGI, Active Networks, Network Security
- DoE Proposals: NGI

NGI-Related Technology Transfer

Test and Measurement Technology for NGI

- QoS Sensitivity Analysis, Experimentation and Measurement Tools
  NIST Net and ISPI
- Network Protocol Test Systems
  IPsec WIT and DIPPER (a distributed QoS test system)

Research Prototypes of Emerging NGI Standards

- IP Security Prototype: Cerberus
- Multi-Protocol Label Switching Prototype: NIST Switch

Leadership in Industry Standards for NGI

- Creating Next-Generation Encryption: AES
- Lead Author on Five IP Security Specifications: IETF
- Building Consensus on Fair Access: IEEE 802.14 HFC
- Pushing for Reconfigurable Optical Networks: OIF

Summary

NIST transfers technology from government-funded research to commercial products and services for the NGI:

- by collaborating with industry to establish standards for the NGI
- by developing and distributing advanced test and measurement technology and research prototypes of emerging NGI standards
- by applying emerging NGI technology to assist the U.S. manufacturing sector